PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS AND INTERFERENCES

In re the Application of:
Berson et al.

Group Art Unit:
3621

Application No.:
09/596,857

Examiner:
Wang, Mary Da Zhi

Filed:
06/19/2000

Docket No.:
A0460Q-US-NP

For: **SYSTEM, METHOD AND ARTICLE OF MANUFACTURE FOR CRYPTOSERVER-BASED AUCTION**

BRIEF ON APPEAL

Appeal from Group 3621
XEROX Corporation

Daniel B. Curtis
Telephone: (650) 812-4259
Attorney for Appellants

Docket No.: A0460Q-US-NP

Application No.: 09/596,857

TABLE OF CONTENTS

Page

I. Introduction 1

II. Real party in interest 1

III. Related appeals and interferences 1

IV. Status of claims 1

V. Status of amendments 3

VI. Summary of claimed subject matter 3

A. Independent claims 1, 11 and 15 3

B. Dependent claims 2, 12 and 16 4

C. Dependent claims 3 and 17 5

D. Dependent claim 10 5

E. Dependent claims 4 and 18 5

F. Dependent claims 5, 13 and 19 5

G. Dependent claims 6, 14 and 20 5

H. Dependent claim 24 6

I. Dependent claims 7 and 21 6

J. Dependent claims 8 and 22 6

K. Dependent claims 9 and 23 6

VII. Grounds of rejection to be reviewed on appeal 6

VIII. Argument 7

A. Whether claims 1-5, 9, 11-13, 15-19 and 23 are properly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663). 7

B. Whether claims 1-5, 9, 11-13, 15-19 and 23 are patentable under 35 U.S.C. §103(a) as being non-obvious over Yamamoto (6,078,663). 16

C. Whether claims 6-8, 14, 20-22 and 24 are properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Coyle (6,269,157). 17

1. The asserted combination of references fails to teach the claimed invention. 18
2. There is no motivation or suggestion in the prior art to make the asserted combination of references. 19

D. Whether claim 10 is properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Schneier (5,956,404). 20
1. The asserted combination of references fails to teach the claimed invention. 21
2. There is no motivation or suggestion in the prior art to make the asserted combination of references. 21

IX. Conclusion 22
X. Claims APPENDIX 1

Docket No.: **A0460Q-US-NP**
Application No.: **09/596,857**

I. Introduction

This is an appeal from an Office Action mailed 4/20/2004, finally rejecting claims 1-24 of the above-identified patent application.

II. Real party in interest

The real party in interest in this appeal in the present application is Xerox Corporation, by way of an assignment recorded at reel/frame 010933/342-343.

III. Related appeals and interferences

There are presently no appeals or interferences, known to Applicant, Applicant's representative or the Assignee, which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

IV. Status of claims

Claims 1–24 are pending in this application.

Pending claims 1–24 are finally rejected in the outstanding Office Action and are on appeal. Of the claims that are on appeal, claims 1 (a method claim), 11 (a computer program product claim) and 15 (a system claim) are independent claims. Claims 2-10 directly or indirectly depend from claim 1. Claims 12-14 depend from claim 11. Claims 16-24 directly or indirectly depend from claim 15. Claims 1– 24 are set forth in the attached Appendix.

Applicant hereby appeals the rejection of claims 1-24.

Claim	Under Appeal Status	Rejected Status	Allowed Status	Withdrawn Status	Objected-to Status	Canceled Status
1	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
2	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
3	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled

Docket No.: **A0460Q-US-NP**

Application No.: **09/596,857**

Claim	Under Appeal Status	Rejected Status	Allowed Status	Withdrawn Status	Objected-to Status	Canceled Status
4	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
5	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
6	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
7	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
8	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
9	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
10	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
11	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
12	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
13	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
14	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
15	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
16	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
17	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
18	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
19	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
20	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
21	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
22	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
23	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled
24	Appealed	Rejected	Not Allowed	Not Withdrawn	Not Objected to	Not Canceled

V. Status of amendments

An Amendment After Final Rejection was filed on 6/21/2004 in response to the final Office Action mailed on 4/20/2004. The After-Final amendment included a replacement drawing for sheet 3/17 (Fig. 1B) in response to an objection to the claim raised in the final Office Action. The 7/13/2004 Advisory Action refused entry of the Amendment After Final Rejection in its entirety as Examiner Cheung did not find applicant's arguments to be persuasive. A notice of appeal and a one month extension was filed on 8/6/2004. No amendments have been filed subsequent to the final rejection. This appeal brief was due on 10/6/04 but faxed on 11/8/04. 11/6/04 falls on a Saturday thus, applicant petitions for a one month extension in accordance with 37 CFR 41.37(e) and 37 CFR 1.136(a)(1), and has included the fee specified in 37 CFR 1.17(a).

VI. Summary of claimed subject matter

A. Independent claims 1, 11 and 15

Claims 1, 11 and 15 are respectively directed to a method, computer program product and system for pricing a "cryptographic service" on a network utilizing one or more cryptoservers.

A cryptoserver is located at a well connected node on a network and is configured to perform CPU intensive cryptographic computations. The cryptoserver may include special purpose hardware devices for performing the cryptographic computations (page 15, lines 19-26).

A "cryptographic service" is a networked service provided to a user that off-loads the burden of performing a "cryptographic operation" (page 18, lines 22-25) from the user to a cryptoserver that performs the "cryptographic operation" for the user (page 16, lines 6-7, 25). (See page 20, lines 30-31 defining a user to include a person, business, computer executing a computer program, etc.)

A "cryptographic service provider" is an operator of a cryptoserver that is used to provide the "cryptographic service" to a user responsive to a request from the user (page 3, line 27 to page 4, line 19; page 15, line 28 to page 16, line 4; page 24, lines 20-21; page 26, lines 23-27).

The "cryptographic service" can be provided in accordance with a contract (page 26, line 29 to page 27, line 2).

This summary of the invention discusses the claimed invention with reference to the elements of independent method claim 1. Since the elements of the system and computer program product claims are substantially similar to the elements of the method claim, the following summary of the claimed invention applies equally to the elements of the computer program product and system claims 11 and 15.

Previously presented claim 1 is directed to a method for pricing a "cryptographic service" (page 20, lines 24-25; page 26, line 20 to page 27, line 2). A user who desires to off-load a "cryptographic operation" from the user can select a "cryptographic service provider" to perform the "cryptographic operation" for the user (by selecting the cryptographic service appropriate for the "cryptographic operation"). The "cryptographic service provider" receives a request for the desired service and generates a contract based on a variable pricing scheme and sends the contract to the user (page 26, line 20 to page 27, line 2; page 20, line 29 to page 22, line 2). Assuming acceptance of the contract, the user sends information to the "cryptographic service provider." The "cryptographic service provider" then causes the contracted-for "cryptographic service" to be applied to the user-supplied information and thus satisfy the contract (Figure 7; page 20, line 24 to page 21, line 14; page 21, lines 14-20; and page 24, lines 19-21). Thus, the user can off-load the burden of performing the "cryptographic service" on the information provided by the user to the cryptographic service.

B. Dependent claims 2, 12 and 16

Dependent claims 2, 12 and 16 further define their respective independent claims by having the "cryptographic service provider" select one of available cryptoservers to perform the contracted-for "cryptographic service" (original claim 2).

C. Dependent claims 3 and 17

Dependent claims 3 and 17 further define claims 2 and 16 respectively further requiring that the "cryptographic service provider" be a commercial service that is competing for customers (original claim 3).

D. Dependent claim 10

Claim 10 depends from claim 3 and wherein the "cryptographic service provider" provides a receipt upon performing the "cryptographic service," where the receipt includes at least one of a one-way hash of the results of its computations, the time and duration of the computations, a description of the computations, and the identities of the one or more cryptoservers and the customer (original claim10).

E. Dependent claims 4 and 18

Dependent claims 4 and 18 further define claims 2 and 16 respectively further requiring that the one or more cryptoservers be part of a single distributed service (original claim 4).

F. Dependent claims 5, 13 and 19

Dependent claims 5, 13 and 19 further define their respective independent claims by requiring that the variable pricing scheme be based on one or more factors. These factors include a data load of the one or more cryptoservers during performance of the "cryptographic service," a distance between the one or more cryptoservers and the user, a congestion of the network during performance of the "cryptographic service," and a rating of the one or more cryptoservers performing the "cryptographic service" (original claim 5).

G. Dependent claims 6, 14 and 20

Dependent claims 6, 14 and 20 further define their respective independent claims by requiring that the variable pricing scheme be auction based (original claim 6).

H. Dependent claim 24

Dependent claims 24 depends on and further defines claim 20 wherein the auction-based variable pricing scheme is conducted securely as a cryptographic protocol by some of the one or more cryptoservers (original claim 24 (sense amended to depend from claim 20).

I. Dependent claims 7 and 21

Dependent claims 7 and 21 further define claims 6 and 20 respectively by requiring that the "cryptographic service provider" receives bids for performing the "cryptographic service" from the user (original claim 7).

J. Dependent claims 8 and 22

Dependent claims 8 and 22 further define claims 6 and 20 respectively by requiring that the one or more "cryptographic service providers" bid for providing the "cryptographic service" (original claim 8).

K. Dependent claims 9 and 23

Dependent claims 9 and 23 further define their respective independent claims by requiring that the "cryptographic service provider" is a cryptoserver (original claim 9).

VII. Grounds of rejection to be reviewed on appeal

- Whether claims 1-5, 9, 11-13, 15-19 and 23 are properly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663).
- Whether claims 1-5, 9, 11-13, 15-19 and 23 are patentable under 35 U.S.C. §103(a) as being non-obvious over Yamamoto (6,078,663).
- Whether claims 6-8, 14, 20-22 and 24 are properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Coyle (6,269,157).
- Whether claim 10 is properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Schneier (5,956,404).

Docket No.: **A0460Q-US-NP**

Application No.: **09/596,857**

VIII. Argument

A. Whether claims 1-5, 9, 11-13, 15-19 and 23 are properly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663).

a. Claims 1, 11 and 15

For a prior art reference to anticipate a claim, the reference must disclose each and every element of the claim with sufficient clarity to prove its existence in the prior art. *See In re Spada*, 911 F.2d 705, 708, 15 USPQ 2d 1655, 1657 (Fed. Cir. 1990) ([T]he [prior art] reference must describe the applicant's claimed invention sufficiently to have placed a person of ordinary skill in the field of the invention in possession of it. (citations omitted)). Although this disclosure requirement presupposes the knowledge of one skilled in the art of the claimed invention, that presumed knowledge does not grant a license to read into the prior art reference teachings that are not there. ***Motorola, Inc. v. Interdigital Tech. Corp.***, 43 USPQ 2d 1481, 1490 (Fed. Cir. 1997)

To recap the claimed invention, the user contracts with a "cryptographic service provider" for a "cryptographic service" to be supplied by the "cryptographic service provider," provides information to the "cryptographic service provider" to which the "cryptographic service" is to be applied, and the "cryptographic service provider" then uses a cryptoserver to apply the contracted-for "cryptographic service" to the information provided by the user.

The method aspect of the invention is captured in previously presented Claim 1:

1. A method for pricing a cryptographic service on a network utilizing one or more cryptoservers, comprising:

(a) receiving a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request; and

(c) sending the contract from the cryptographic service provider to the user utilizing the network;

(d) receiving, by the cryptographic service provider, information from the user; and

(e) applying the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

In the final office action dated 04/20/2004 the Examiner has cited Yamamoto Column 16, Lines 20-41; Figures 4 and 11; and the abstract as teaching steps (d) and (e) of claim 1. During the interview with the Examiner of 5/7/04, applicant was unable to convince the Examiner that step (d) of receiving information from the user was not related to the user replying to the contract sent in step (c). The information from the user that is received in step (d) is used in step (e) when the "cryptographic service" the user has contracted-for is applied to the user-supplied information.

According to paragraph 10 of this final office action, the Examiner interprets the "cryptographic service provider" as Yamamoto's "information providing center". Applicants respectfully, but strongly, disagree with the Examiner's interpretation. As will be seen, Yamamoto's "information providing center" provides information that is stored at the "information providing center" to a user at a price that depends on the amount of provided information and the rate the information is enciphered when providing the information. The "cryptographic service provider" of the invention applies the contracted-for "cryptographic service" to information provided by the user, not to information that is available to the "cryptographic service provider" prior to the user's information being received by step (d). Applicants respectfully believe that this mistaken interpretation is a fundamental flaw in the Examiner's understanding of the instant application.

Turning now to the teachings of Yamamoto.

Yamamoto teaches techniques for distributing encrypted information from an "information providing center" to a user who has agreed to a fee for the providing of the information as well as the rate the information is enciphered to protect the provided information. As will be seen, the information being provided is stored at the "information providing center".

Yamamoto teaches: 1) a database at the "information providing center" containing the information (see citations below); 2) agreeing for information from the database to be enciphered at a specified rate (Column 36, Lines 18-24), and 3) providing the enciphered information (see citations below).

Looking now to Yamamoto references provided by the Examiner: Yamamoto Column 16, Lines 20-41; Figures 4 and 11; and the Abstract:

Yamamoto Figure 4 shows the information providing center 40 and is described as:

> "An explanation of an information providing service that employs the above enciphering system follows. A cryptographic communication network that performs the information providing service is constituted by an information providing center and users A, B, . . . , and M, as is shown in FIG. 4. The information providing center 40 and the users A through M employ in common inherent and secret keys that are provided in advance. The key string K_A, K_B, . . . , and K_M comprises respectively the key that is used in common by the information providing center 40 and user A, the key that is used in common by the information providing center 40 and user B, . . . , and the key that is used in common by the information providing center 40 and user M." (Column 10, Lines 8-20; Column 11, Lines 33-36).

As is seen from the citations below, the information providing service 40 provides data that is *stored on the* "information providing service" 40 to a user in enciphered form for a fee:

> "*To provide information for the user A from the information providing center 40* while using the above described enciphering system, the information providing service employs the following procedures." (Column 10, Lines 31-34, emphasis added).
>
> "A user will pay the *information providing center 40* an information providing service fee in consonance with the type, the quality and the quantity of the *information that is provided*." (Column 11, Lines 56-59, emphasis added).

> "When the user A in FIG. 4 specific[sic] information from the information providing center 40, the information providing center 40 *transmits the requested information to the user A*, and in accordance with the following procedures, charges the user a fee for *the information providing service*." (Column 15, Lines 53-57, emphasis added).
>
> "While these keys are being updated, they are employed as keys for block cryptography to encipher information that is provided by the block encipherer 30. The *enciphered information is then transmitted to the user A*." (Column 10, Lines 45-58, emphasis added)

Yamamoto figure 4 and the associated text (as sampled above) clearly show that Yamamoto teaches an "information providing service" that provides information stored at the service to a user in enciphered form where the user is able to contract for which information is stored on the service and for the rate the information is enciphered to protect the information. Neither Yamamoto figure 4 or its associated text teach a "cryptographic service," a cryptoserver, a "cryptographic service provider" or receiving information from the user and applying a "cryptographic service" to that information.

Yamamoto figure 11 teaches an Information Providing Center 40 as used in one embodiment:

> "As is shown in FIG. 11, the information providing center 40 comprises at least each of the following components: the communication terminal 50; a database 41, wherein information *to be provided is stored*; an accounting device 42, for calculating a charge *for each quantity unit of information that is provided*; and a storage device 43, wherein are stored the secret keys of all the users, which are required for cryptographic communication, and service fee information. In FIG. 11, a plurality of communication terminals 50 are provided to enable the simultaneous transmission of information to a plurality of users. *For a larger*

> *information providing system, more than one database 41*, accounting device 42 and storage device 43 may be provided.
>
> In the database 41 that is designed as is shown in FIG. 12 are stored *information that is to be provided for users* and a corresponding charge for an information quantity unit." (Column 14, Lines 23-38, emphasis added).

Yamamoto figure 11 and the associated text (as sampled above) clearly show that Yamamoto teaches an "information providing service" that provides information stored at the service to a user in an enciphered form where the user is able to contract for which information is stored on the service and for the rate of the information is enciphered. Neither Yamamoto figure 11 or its associated text teach a "cryptographic service," a cryptoserver, a "cryptographic service provider" or receiving information from the user and applying a "cryptographic service" to that information.

The Yamamoto Abstract is:

> "A communication device according to the present invention comprises an enciphering transmitter for enciphering data and transmitting enciphered data, a counter for obtaining a count of a quantity of enciphered data, and an accounting circuit for calculating, in accordance with the count held by the counter, an amount to charge a user for the data."

The Yamamoto Abstract does not teach a "cryptographic service," a cryptoserver, a "cryptographic service provider" or receiving information from the user and applying a "cryptographic service" to that information.

Yamamoto Column 16, Lines 20-41 is:

> "Information Providing Preprocedures of the Present Invention
>
> 1. The user A requests that the information providing center 40 provide for the service for Info, detailing at the same time that part of the information

that is desired.

2. Upon the request from the user A that the service for Info be provided, the information providing center 40 calculates a charge for the information providing service by using the unit charge UC_{Info} for Info and the part of the information that is requested by the user, and transmits the obtained service fee information to the user A. When the user A employs the communication terminal 60 shown in FIG. 9, the unit charge UC_{Info} is also transmitted to the user A.

3. If the user A agrees with the received service fee information relative to the requested part of Info, the user A requests that the information providing center 40 provide the service for Info. When the user A employs the communication terminal 60 shown in FIG. 11, the received unit charge UC_{Info} is held in the buffer 57.

If the user does not agree with the received service fee information, the user requests that the information providing center 40 cancel the service for Info, and this procedure is thereafter terminated."

The above cited text teaches that a user of Yamamoto's system requests that Yamamoto's "information providing center" provide identified information. Yamamoto's "information providing center" calculates a service fee for the information and transmits the service fee to the user. The user received the identified information if the user is willing to pay the service fee.

The Examiner cited Yamamoto Column 16, Lines 20-41 as teaching steps (d) and (e) of claim 1 of the instant invention. One skilled in the art could not interpret this as teaching:

(d) receiving, by the cryptographic service provider, information from the user; and

(e) applying the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

Thus, the cited text does not teach a "cryptographic service," a cryptoserver, a "cryptographic service provider" or receiving information from the user and applying a "cryptographic service" to that information.

The invention of claim 1 includes the limitations of elements (d) and (e). That is, that the "cryptographic service provider" receives information *from the user* and that the contracted-for "cryptographic service" be applied to *this information* to satisfy the contract.

While the claims must be given their broadest *reasonable* interpretation by the Examiner, the Examiner must apply the broadest reasonable meaning of the words in their ordinary usage as they would be understood by one of ordinary skill in the art, taking into account whatever enlightenment by way of definitions or otherwise that may be afforded by the written description contained in the applicant's specification. (MPEP 2111).

The Examiner's position that limitations (d) and (e) somehow apply to the *contract* sent by the "cryptographic service provider" to the user is not supported by the plain meaning of the words in the claim. In particular, limitations (d and e) "receiving, by the "cryptographic service provider," information from the user and applying the "cryptographic service" to the information using the one or more cryptoservers to satisfy the contract" clearly require that the user send information to the "cryptographic service provider" and that the contracted-for "cryptographic service" is applied to that information to satisfy the contract. At no point in the claims or in the specification is there a suggestion that the contract is the information that is being operated on by the "cryptographic service." In addition, applicant respectfully asserts that one skilled in the art would find the Examiner's interpretation to be unreasonable.

Furthermore, nothing in Yamamoto teaches or enables a "cryptographic service," a cryptoserver, a "cryptographic service provider" or receiving information from the user and applying a contracted-for "cryptographic service" to that information. Thus, Yamamoto does not anticipate the invention of claim 1. Thus, claim 1 was improperly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663).

The computer program aspect of the invention is captured by claim 11. Claim 11 is not anticipated for substantially the same reasons that claim 1 is not anticipated. Thus, claim 11 was improperly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663).

The system aspect of the invention is captured by claim 15. Claim 15 is not anticipated for substantially the same reasons that claim 1 is not anticipated (logic (f) and (g) in claim 15 perform operations that perform the steps (d) and (e) in claim 1). Thus, claim 15 was improperly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663).

Thus, claims 1, 11 and 15 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

Claims 2, 12 and 16 depend on and further limit their respective parent claims. Thus, claims 2, 12 and 16 are not anticipated. In addition, nothing in Yamamoto teaches a "cryptographic service," a cryptoserver, a "cryptographic service provider" or contracting with a "cryptographic service provider" to obtain a "cryptographic service" performed on a cryptoserver. Thus, claims 2, 12 and 16 were improperly rejected under 35 U.S.C. 102(e) and applicant appeals to have this rejection reversed.

Claims 3 and 17 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches a "cryptographic service provider." Thus, claims 3 and 17 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claim10 depends on and further limits claim 3 that is not anticipated. In addition, nothing in Yamamoto teaches a "cryptographic service provider" or a cryptographic service. Thus, claim 10 is not anticipated and were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claims 4 and 18 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches a cryptoserver. Thus, claims 4 and 18 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claims 6, 14 and 20 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches an auction based pricing scheme. Thus, claims 6, 14 and 20 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claim 24 depends on and further limits its parent claim. In addition, nothing in Yamamoto teaches an auction based pricing scheme or a cryptoserver. Thus, claim 24 is not anticipated and this claim was improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claims 7 and 21 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches a "cryptographic service," a "cryptographic service provider" or receiving bids from the user for performing the cryptographic service. Thus, claims 6, 14 and 20 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claims 8 and 22 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches a "cryptographic service," a "cryptographic service provider" or providing bids from the "cryptographic service provider" for performing the cryptographic service. Thus, claims 8 and 22 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

Claims 9 and 23 depend on and further limit their respective parent claims. In addition, nothing in Yamamoto teaches a cryptoserver or a "cryptographic service provider." Thus, claims 9 and 23 are not anticipated and these claims were improperly rejected under 35 U.S.C. 102(e). Thus, applicant appeals to have this rejection reversed.

For these reasons, claims 1-5, 9, 11-13, 15-19 and 23 were improperly rejected under 35 U.S.C. §102(e) as anticipated by Yamamoto (6,078,663) and applicant respectfully requests reversal of this 35 U.S.C. §102(e) rejection.

B. Whether claims 1-5, 9, 11-13, 15-19 and 23 are patentable under 35 U.S.C. §103(a) as being non-obvious over Yamamoto (6,078,663).

Applicant addresses the issue of non-obviousness of Claims 1, 11, and 15 with respect to Yamamoto to help advance the prosecution of the instant application towards allowance.

In rejecting claims under 35 U.S.C. §103(a), the Patent Office bears the initial burden of persuasion in establishing a prima facie case of obviousness. To achieve this, the Patent Office must show three criteria: a suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine teachings; a reasonable expectation of success; and that the prior art must teach or suggest all claimed limitations. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). See also MPEP §2143.

Having discussed the invention of claims 1, 11 and 15; and having discussed the teachings of Yamamoto; nothing in Yamamoto would have enabled one skilled in the art to make and use the method of claim 1, make and use the program product of claim 11 or make and use the system of claim 15.

The problem addressed by the invention of claims 1, 11 and 15 is that of off-loading the burden of performing a "cryptographic operation" from the user to a cryptoserver that performs the "cryptographic operation" for the user (page 20, line 31 to page 21, line 5). The "cryptographic service" is provided to the user in accordance with a contract.

With respect, the Examiner's interpretation of Yamamoto's "information providing center 40" as reading on a "cryptographic service provider" is clearly a mistaken interpretation. In addition, the Examiner's interpretation that the information sent by the user by step (d) is related to the contract is inconsistent with the plain reading of step (e) that requires that the "cryptographic service" is applied to the information provided in step (d) to satisfy the contract.

Yamamoto does not address the problem addressed by the claimed invention. Yamamoto teaches techniques for distributing encrypted information from an "information providing center" to a user who has agreed to a fee for the providing of the information as well as the rate the

information is enciphered when providing the information. The information is stored at the "information providing center".

Yamamoto teaches: 1) a database at the "information providing center" containing the information; 2) agreeing for information from the database to be enciphered at a specified rate, and 3) providing the data so encrypted.

Nothing in Yamamoto teaches a "cryptographic service," a cryptoserver, a "cryptographic service provider" or contracting with a "cryptographic service provider" to obtain a "cryptographic service" performed by a cryptoserver.

Furthermore, Yamamoto does not teach a suggestion, nor show a motivation that would enable one skilled in the art to make or use a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Thus, claims 1, 11 and 15 are non-obvious over Yamamoto. Claims 2-10, 11-14, and 16-24 depend on and further limit, directly or indirectly, their respective independent claims that are patentable over Yamamoto. For at least this reason, claims 2-10, 11-14, and 16-24 are non-obvious over Yamamoto.

C. Whether claims 6-8, 14, 20-22 and 24 are properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Coyle (6,269,157).

The Yamamoto reference has been previously discussed with respect to independent claims 1, 11 and 15, and dependent claims 2-10, 11-14, and 16-24.

The Coyle reference teaches a computerized bidding system for selecting telecommunication carriers through an auction (Coyle, Column 9, Lines 13-16). The bid information can be encrypted (Coyle, Column 13, Lines 30-45). Coyle addresses the problem of electronically determining the best carrier for telecommunications balancing cost, available capacity, and quality of service.

Coyle does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Coyle does not teach the limitations within steps (d) or (e) of claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

1. **The asserted combination of references fails to teach the claimed invention.**

As previously discussed, Yamamoto does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Yamamoto does not teach the limitations within steps (d) or (e) of claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

Coyle does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Coyle does not teach the limitations within steps (d) or (e) of claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

Thus, the combination of Yamamoto and Coyle does not teach the invention of independent claims 1, 11 and 15. Claims 6-8, 14, 20-22 and 24 depend on and further limit one of independent claims 1, 11 and 15 either directly or through intervening claims. Thus, the

combination of Yamamoto and Coyle does not teach the invention of claims 6-8, 14, 20-22 and 24.

2. **There is no motivation or suggestion in the prior art to make the asserted combination of references.**

The reason to make the asserted combination of references must stem from some teaching, suggestion or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. Uniroyal Inc. v. F-Wiley Corp., 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed. Cir. 1988), cert. denied, 488 U.S. 825 (1988); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 293, 227 USPQ 657, 664 (Fed. Cir. 1985), cert. denied, 475 U.S. 1017 (1986); ACS Hospital Systems, Inc. v. Montefiore Hospital, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed. Cir. 1984). These showings by the examiner are an essential part of complying with the burden of presenting a prima facie case of obviousness.

Nothing in Yamamoto would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Nothing in Coyle would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Nothing in the combination of Yamamoto and Coyle would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a

cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Thus, the combination of Yamamoto and Coyle would not motivate nor suggest to one skilled in the art the invention of independent claims 1, 11 and 15. Claims 6-8, 14, 20-22 and 24 depend on and further limit one of independent claims 1, 11 and 15 either directly or through intervening claims. Thus, the combination of Yamamoto and Coyle would not motivate nor suggest to one skilled in the art the invention of the invention of claims 6-8, 14, 20-22 and 24.

Thus, a prima facie case for obviousness of claims 6-8, 14, 20-22 and 24 has not been made and applicant respectfully requests reversal of the 35 U.S.C. §103(a) rejection of these claims.

D. Whether claim 10 is properly rejected under 35 U.S.C. §103(a) as being unpatentable over Yamamoto in view of Schneier (5,956,404).

The Schneier reference teaches method of creating a digital signature and discloses public-key encryption, digital signatures, and one-way hash functions that are well known in the art.

Schneier does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Schneier does not teach the limitations within steps (d) or (e) of the claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

1. **The asserted combination of references fails to teach the claimed invention.**

Schneier does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Schneier does not teach the limitations within steps (d) or (e) of the claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

Yamamoto does not teach a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider." In particular, Yamamoto does not teach the limitations within steps (d) or (e) of the claims 1 or 11, or the limitations of logic (f) and (g) in claim 15 (that perform the steps (d) and (e) in claim 1).

Thus, the combination of Yamamoto and Schneier does not teach the invention of independent claims 1, 11 and 15. Claim 10 depends on and further limits independent claim 1 through intervening claims 3 and 2. Thus, the combination of Yamamoto and Schneier does not teach the invention of claim 10.

2. **There is no motivation or suggestion in the prior art to make the asserted combination of references.**

Nothing in Yamamoto would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by

the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Nothing in Schneier would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Nothing in the combination of Yamamoto and Schneier would motivate or suggest to one skilled in the art a "cryptographic service" that would allow a user to off-load the burden of performing a "cryptographic operation," on information provided by the user, from the user to a cryptoserver; where the cryptoserver performs the "cryptographic operation" on the information provided by the user in accordance with a contract for the "cryptographic service" between the user and the "cryptographic service provider."

Thus, the combination of Yamamoto and Schneier would not motivate nor suggest to one skilled in the art the invention of independent claims 1, 11 and 15. Claim 10 depends on and further limits independent claim 1 through intervening claims 3 and 2. Thus, the combination of Yamamoto and Schneier would not motivate nor suggest to one skilled in the art the invention of the invention of claim 10.

Thus, a prima facie case for obviousness of claim 10 has not been made and applicant respectfully requests reversal of the 35 U.S.C. §103(a) rejection of claim 10.

IX. Conclusion

For at least the reasons discussed above, it is respectfully submitted that claims 1–24 contain patentable subject matter and are distinguishable over the applied references.

Docket No.: **A0460Q-US-NP**
Application No.: **09/596,857**

Applicant respectfully requests the Honorable Board to reverse the final rejection of the claims and return the application to the Examiner to pass this case to issue.

Respectfully submitted,

Daniel B. Curtis
Attorney for Applicant(s)
Registration No. 39,159
Telephone: 650-812-4259

Date: November 8, 2004

Attachment: Appendix of Claims

Docket No.: A0460Q-US-NP
Application No.: 09/596,857

X. Claims APPENDIX

Claim 1 (previously presented): A method for pricing a cryptographic service on a network utilizing one or more cryptoservers, comprising:

(a) receiving a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) generating a contract based on a variable pricing scheme in response to the request;

(c) sending the contract from the cryptographic service provider to the user utilizing the network;

(d) receiving, by the cryptographic service provider, information from the user; and

(e) applying the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

Claim 2 (previously presented): The method as recited in claim 1, wherein the cryptographic service provider selects one of the one or more cryptoservers to perform the cryptographic service.

Claim 3 (previously presented): The method as recited in claim 2, wherein the cryptographic service provider is a commercial service competing for customers.

Claim 4 (previously presented): The method as recited in claim 2, wherein the one or more cryptoservers is part of a single distributed service.

Claim 5 (previously presented): The method as recited in claim 1, wherein the variable pricing scheme is based on at least one of a data load of the one or more cryptoservers during performance of the cryptographic service, a distance between the one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the one or more cryptoservers performing the cryptographic service.

Claim 6 (original): The method as recited in claim 1, wherein the variable pricing scheme is auction-based.

Claim 7 (original): The method as recited in claim 6, wherein the cryptographic service provider receives bids for performing the cryptographic service from the user.

Claim 8 (previously presented): The method as recited in claim 6, wherein the one or more cryptoservers bid for providing the cryptographic service.

Claim 9 (previously presented): The method as recited in claim 1, wherein the cryptographic service provider is one of the one or more cryptoservers.

Claim 10 (previously presented): The method as recited in claim 3, wherein the cryptographic service provider provides a receipt upon performing the cryptographic service, wherein the receipt includes at least one of a one-way hash of the results of its computations, the time and duration of the computations, a description of the computations, and the identities of the one or more cryptoservers and the customer.

Claim 11 (previously presented): A computer program embodied on a computer readable medium for pricing a cryptographic service on a network utilizing one or more cryptoservers, comprising:

(a) a code segment that receives a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(b) a code segment that generates a contract based on a variable pricing scheme in response to the request;

(c) a code segment that sends the contract from the cryptographic service provider to the user utilizing the network;

(d) a code segment that receives, by the cryptographic service provider, information from the user; and

(e) a code segment that applies the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

Claim 12 (previously presented): The computer program as recited in claim 11, wherein the cryptographic service provider selects one of the one or more cryptoservers to perform the cryptographic service.

Claim 13 (previously presented): The computer program as recited in claim 11, wherein the variable pricing scheme is based on at least one of a data load of the one or more cryptoservers during performance of the cryptographic service, a distance between the one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the one or more cryptoservers performing the cryptographic service.

Claim 14 (original): The computer program as recited in claim 11, wherein the variable pricing scheme is auction-based.

Claim 15 (previously presented): A system for pricing a cryptographic service comprising:

(a) a network;

(b) one or more cryptoservers for providing a cryptographic service;

(c) logic that receives a request for the cryptographic service from a user utilizing the network, wherein the request is received by a cryptographic service provider;

(d) logic that generates a contract based on a variable pricing scheme in response to the request;

(e) logic that sends the contract from the cryptographic service provider to the user utilizing the network;

(f) logic that receives, by the cryptographic service provider, information from the user; and

(g) logic that applies the cryptographic service to the information using the one or more cryptoservers to satisfy the contract.

Claim 16 (previously presented): The system as recited in claim 15, wherein the cryptographic service provider selects one of the one or more cryptoservers to perform the cryptographic service.

Claim 17 (previously presented): The system as recited in claim 16, wherein the cryptographic service provider is a commercial service competing for customers.

Claim 18 (previously presented): The system as recited in claim 16, wherein the one or more cryptoservers is part of a single distributed service.

Claim 19 (previously presented): The system as recited in claim 15, wherein the variable pricing scheme is based on at least one of a data load of the one or more cryptoservers during performance of the cryptographic service, a distance between the one or more cryptoservers and the user, a congestion of the network during performance of the cryptographic service, and a rating of the one or more cryptoservers performing the cryptographic service.

Claim 20 (original): The system as recited in claim 15, wherein the variable pricing scheme is auction-based.

Claim 21 (original): The system as recited in claim 19, wherein the cryptographic service provider receives bids for performing the cryptographic service from the user.

Claim 22 (previously presented): The system as recited in claim 19, wherein the one or more cryptoservers bid for providing the cryptographic service.

Claim 23 (previously presented): The system as recited in claim 15, wherein the cryptographic service provider is one of the one or more cryptoservers.

Claim 24 (previously presented): The system as recited in claim 20, wherein the auction-based variable pricing scheme is conducted securely as a cryptographic protocol by some of the one or more cryptoservers.